PCT/CN03/00801

证　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2002 10 18

申　请　号：　02 1 44191.X

申请类别：　发明

发明创造名称：　一种网络安全认证方法

申　请　人：　华为技术有限公司

发明人或设计人：张涛；张忠

中华人民共和国
国家知识产权局局长　王景川

2003 年 10 月 14 日

权 利 要 求 书

1、一种网络安全认证方法，包括下述步骤：

步骤1：媒体网关控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包；

步骤2：在进行安全认证时，MGC利用数据包(Package)向MG下发安全认证请求数据，MG利用鉴权密钥对请求数据进行加密计算，并将计算结果反馈给MGC；

步骤3：MGC根据认证结果确定被认证的MG是否合法。

2、根据权利要求1所述的网络安全认证方法，其特征在于：所述网络协议为媒体网关控制协议（MGCP）。

3、根据权利要求1所述的网络安全认证方法，其特征在于：所述网络协议为H248协议。

4、根据权利要求1、2或3所述的网络安全认证方法，其特征在于，所述数据包包括：安全认证请求信号和安全认证结果事件；所述安全认证请求信号中包括安全认证参数；安全认证结果事件中包括安全结果认证参数。

5、根据权利要求4所述的网络安全认证方法，其特征在于，所述步骤2进一步包括：

步骤21：MGC下发数据包中的安全性认证请求信号给MG；

步骤22：MG收到安全认证信号中的安全认证参数，使用鉴权密钥对上述参数进行加密计算，然后将加密计算结果通过数据包中的安全认证完成事件

02·10·23

的安全结果认证参数上报给MGC。

6

说　　明　　书

一种网络安全认证方法

技术领域

本发明涉及一种网络的安全认证方法。

背景技术

在下一代网络（NGN）中，存在很多基于媒体网关控制协议（MGCP）和H248协议（另一种媒体网关控制协议）的媒体网关（MG），这些设备分布在企业或用户家中，具有面广、量大、基于动态IP的特点。但在目前的NGN网络中，由于MGCP协议的应用层无安全认证机制，所以使用MGCP协议的MG安全性较差；在H248协议中，尽管在应用层中有安全认证机制，即在每个H248协议事务请求消息中可以加入安全头，在其事务响应消息中返回安全认证结果，但是该安全认证机制要在MGC和MG中要交互大量H248消息，大约要增加40%的H248消息编解码处理时间，这使得现有的H248协议提供的安全认证方案大大降低了网络系统的效率，实际应用的可行性较差。因此，目前NGN网络存在的仿冒MG，对MGC进行攻击等系统安全问题还没有得到妥善的解决。

发明内容

本发明的目的在于提供一种能够对NGN网络进行有效的安全认证的方法。

为达到上述目的，本发明提供的网络安全认证方法，包括：

步骤1：媒体网关控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包；

步骤2：在进行安全认证时，MGC利用数据包(Package)向MG下发安全认证请求数据，MG利用鉴权密钥对请求数据进行加密计算，并将计算结果反馈给MGC；

步骤3：MGC根据认证结果确定被认证的MG是否合法。

所述网络协议为媒体网关控制协议（MGCP）或H248协议。

所述数据包包括：安全认证请求信号和安全认证结果事件；所述安全认证请求信号中包括安全认证参数；安全认证结果事件中包括安全结果认证参数。

所述步骤2进一步包括：

步骤21：MGC下发数据包中的安全性认证请求信号给MG；

步骤22：MG收到安全认证信号中的安全认证参数，使用鉴权密钥对上述参数进行加密计算，然后将加密计算结果通过数据包中的安全认证完成事件的安全结果认证参数上报给MGC。

由于本发明采用媒体网络控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包用于MG的安全认证，因此能够防止非法和伪造设备的网络接入；另外，由于对MG的认证在MGC的控制下进行，或

者说在MGC认为需要安全认证的时候进行安全认证，这样的认证方式具有随机性，具有较高的安全认证效率。

具体实施方式

下面结合附图对本发明作进一步详细的描述。

本发明所述的方法是实现MG的安全管理，其实质是，为每一个MG配置一个鉴权密钥，当MGC发起鉴权请求时，MGC将向MG发一个随机数，MG根据MGC发来的随机数和MG配置的鉴权密钥（当然还可以包括其他信息），实施加密计算，返回加密结果给MGC。MGC实施相同的计算，判断是否与MG发送的加密结果相同。如果不相同则认为MG为非法。

本发明可以基于H248协议或MGCP协议实现，为此需要增加MGCP协议或H248协议安全数据包，所述安全性数据包是安全性认证信号和事件的集合，本发明采用的H248协议或MGCP协议的安全性认证包中包括一个安全性认证请求信号和安全性认证完成事件。安全认证请求信号中包括一个安全性认证参数；安全性完成事件中包括一个安全性认证结果参数。当MGC要对MG进行安全性认证时，MGC下发安全性认证请求信号给MG，同时检测MG的安全性认证完成事件。当MG收到MGC下发的安全性认证信号，根据配置在MG上的鉴权密钥和收到的MGC安全性认证请求信号中的参数进行加密计算。当完成加密计算，MG向MGC上报安全性认证完成事件，在安全性认证完成事件的参数中上报安全加密计算结果。MGC收到MG上报的安全性

认证完成事件后，比较MG上报的安全性认证完成事件参数中的加密计算结果是否与MGC本身计算的加密结果相同。如果不相同则认为是非法的MG。

下面举例说明上述过程。

采用MGCP协议实现本发明的MGCP协议安全数据包具体内容为：

数据包名称：Auth；数据包版本：1；

包中包含的事件：

1：安全认证结果事件

事件名称：authoc；

检测事件参数编码：32*64(十六进制数)；

说明： 检测事件参数用于返回认证结果；

包中包含的信号：

1：安全认证请求信号

信号名编码：authreq；

信号参数编码：32*64(十六进制数32到64位）；

上述安全认证请求信号参数即为MGC向MG发出的一个随机数。本例中，随机数为大于16位的字符串小于32位的字符串。每一位字符串ABNF（扩展的巴科斯范式）编码为2个十六进制数。

基于上述数据包的认证过程及采用的伪代码为：

步骤11：MGC向MG发起认证请求：MGC下发请求通知命令（RQNT）给MG，分配事务标识（100）和请求标识（123），要求MG检测安全认证完

成事件（auth/authoc），同时下发安全认证请求信号（auth/authreq），MGC生成一个16字节的随机数（0x78 0x90 0xab 0xcd 0xef 0x56 0x78 0x90 0x00 0x22 0x00 0x22 0x00 0x22 0x00 0x32)作为安全认证请求信号的安全认证参数。

步骤12：MG收到MGC下发的请求通知命令（RQNT）后回送此命令的正确响应，响应码为正确响应（200），事务标识（100）与MGC下发的请求通知（RQNT）命令的事务标识一致。证明MG已正确收到MGC下发的请求通知命令（RQNT）。

步骤13：MG收到MGC下发的请求通知命令（RQNT）后发现有安全认证请求信号，开始进行安全认证计算，MG取出安全认证请求信号中的参数和配置在MG上的鉴权密钥（该鉴权密钥假设为：0x12 0x24 0x56 0x78 0x56 0x32 0x78 0x23 0x24 0x25 0x76 0x32 0x32 0x45 0x45 0x32）进行加密计算。经加密计算，加密计算结果为（0x12 0x 34 0xab 0xcd 0xef 0xab 0xef 0x90 0x00 0x22 0x00 0x22 0x67 0x89 0x77 0x88），MG产生安全认证完成事件，MG查看是否MGC要求上报加密完成事件，MG发现MGC要求上报该事件，MG上报通知命令（NTFY）给MGC，检测到事件为安全认证完成事件（auth/authoc），事件参数为加密结果。请求标识（123）与MGC下发的请求通知命令（RQNT）的请求标识一致，同时分配事务标识（200）。

步骤14：MGC收到MG上报的通知事件后，回送通知命令的正确响应，响应码为正确响应（200），事务标识（200）与MG上报的通知命令

（NTFY）的事务标识一致。证明MGC已正确收到MG上报的通知命令（NTFY）。

步骤15：当MGC收到MG上报的加密结果，与自己计算的加密结果比较，如果MG上报的加密结果与MGC自己计算的加密结果一致。则认为该MG为合法的MG，如果不一致或者MG在规定的时间内没有上报自己的加密结果，则认为该MG为非法的MG。

采用H248协议实现本发明的H248协议安全数据包为：

数据包名称：auth；数据包版本：1；

数据包中的事件：

1：安全认证结果事件

事件名称：authoc（0x0001）；

检测事件参数名：认证结果；

参数名称：Res；

参数值ABNF编码：32*64(32到64位的16进制数）；

参数值 ASN.1(抽象符号表示法)编码：OCTET STRING(SIZE(16..32))：（16到32位的8位位组）；

数据包中包含的信号：

1：安全认证请求信号

信号名标识：authreq

信号参数名：请求参数

参数名称：parm

参数值ABNF编码：32*64(HEXDIG)

参数值ASN.1编码：OCTET STRING(SIZE(16..32))

基于上述数据包的认证过程及采用的伪代码为

步骤21：MGC向MG发起认证请求：MGC下发请求修改命令（modify）给MG，分配事务标识（100）和请求标识（2223），要求MG检测安全认证完成事件（auth/authoc），同时下发安全认证请求信号（auth/authreq），MGC生成一个16字节的随机数（0x78 0x90 0xab 0xcd 0xef 0x56 0x78 0x90 0x00 0x22 0x00 0x22 0x00 0x22 0x00 0x32)作为安全认证请求信号的安全认证参数。

步骤22：MG收到MGC下发的修改命令（modify）后回送此命令的正确响应，事务标识（10001）与MGC 下发的修改命令（modify）的事务标识一致。证明MG已正确收到MGC 下发的修改命令（modify）。

步骤23：MG收到MGC 下发的修改命令（modify）后发现有安全认证请求信号，开始进行安全认证计算，MG取出安全认证请求信号中的参数和配置在MG上的鉴权密钥（假设该鉴权密钥为：0x12 0x24 0x56 0x78 0x56 0x32 0x78 0x23 0x24 0x25 0x76 0x32 0x32 0x45 0x45 0x32）进行加密计算。经加密计算，加密计算结果为（0x12 0x 34 0xab 0xcd 0xef 0xab 0xef 0x90 0x00 0x22 0x00 0x22 0x67 0x89 0x77 0x88）,MG产生安全认证完成事件，MG查看是否MGC要求上报加密完成事件，MG发现MGC要求上报该事件，MG上报

通知命令（NTFY）给MGC，检测到事件为安全认证完成事件（auth/authoc），事件参数为加密结果。请求标识（2223）与MGC下发的修改命令（modify）的请求标识一致，同时分配事务标识（10002）。

步骤24：MGC收到MG上报的通知事件后，回送通知命令的正确响应，事务标识（10002）与MG上报的通知命令（NTFY）的事务标识一致。证明MGC已正确收到MG上报的通知命令（NTFY）。

步骤25：当MGC收到MG上报的加密结果，与自己计算的加密结果比较，如果MG上报的加密结果与MGC自己计算的加密结果一致。则认为该MG为合法的MG，如果不一致或者MG在规定的时间内没有上报自己的加密结果，则认为该MG为非法的MG。